(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2005年2月3日 (03.02.2005)

PCT

(10) 国際公開番号
WO 2005/010850 A1

(51) 国際特許分類[7]: G09C 1/00, H04L 9/06

(21) 国際出願番号: PCT/JP2004/009907

(22) 国際出願日: 2004年7月6日 (06.07.2004)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2003-273948 2003年7月14日 (14.07.2003) JP

(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒1410001 東京都品川区北品川6丁目7番35号 Tokyo (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 伊藤 雄二郎 (ITO, Yujiro) [JP/JP]; 〒1410001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP). 下里 努 (SHIMOSATO, Tsutomu) [JP/JP]; 〒1410001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP). 辻川 和伸 (TSUJIKAWA, Kazunobu) [JP/JP]; 〒1410022 東京都品川区東五反田2丁目20番4号 ソニー・ヒューマンキャピタル株式会社内 Tokyo (JP).

(74) 代理人: 杉浦 正知, 外(SUGIURA, Masatomo et al.); 〒1710022 東京都豊島区南池袋2丁目49番7号 池袋パークビル7階 Tokyo (JP).

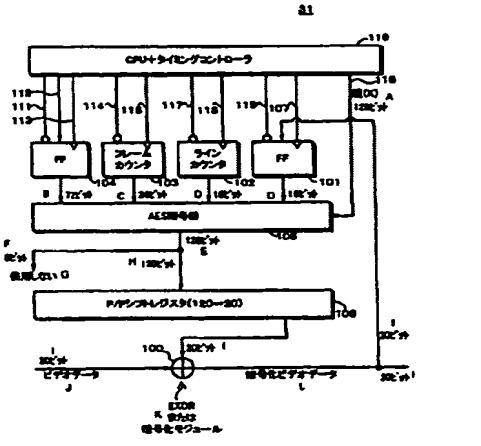
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG,

[続葉有]

(54) Title: ENCRYPTION/DECRYPTION DEVICE AND METHOD

(54) 発明の名称: 暗号/復号装置及び方法



(57) Abstract: It is possible to perform encryption ensuring an excellent confidentiality and capable of completely coming back from an error. Input video data is calculated with pseudo-random numbers by an EXOR (100) and the encrypted data obtained is held by an FF (101) and reset by each line. Counters (102, 103) are incremented by each line and each frame and reset by each frame and a program head, respectively. An encryption device (105) encrypts outputs of an FF (104) for holding a fixed value, counters (103, 102) and the FF (101) by using a key (K) so as to generate pseudo-random numbers and divides a bit string by a shift register (106). The output of the shift register (106) and the input video data are calculated by EXOR (100) to obtain encrypted data. Since the encrypted output is fed back, it is impossible to perform stealing using the continuous input of the same data. Moreover, since the encrypted output which is fed back is reset by each line, it is possible to completely come back from an error.

(57) 要約: 秘守性に優れ、エラーから完全に復帰できる暗号化を行う。入力映像データがＥＸＯＲ１００で疑似乱数列と演算されて得られた暗号化データがＦＦ１０１にホールドされ、ライン毎にリセットされる。カウンタ１０２及び１０３は、夫々ライン毎及びフレーム毎に計数され、フレーム毎及びプログラムの先頭でリセットされる。暗号器１０５は、固定値をホールドするＦＦ１０４、カウンタ１０３、１０２及びＦＦ１０１の出力を鍵（Ｋ）を用いて暗号化して疑似乱数列を発生させ、シフトレジスタ１０６でビット列を分割する。シフトレジスタ１０６の出力と入力映像データとがＥＸＯＲ１００で演算され、暗号化データが得られる。暗号出力をフィードバックするので同一データの連続入力を利用したデータ窃取が行えないと共に、フィードバックする暗号出力がライン毎にリセットされるので、エラーから完全に復帰できる。

BEST AVAILABLE COPY

BEST AVAILABLE COPY

WO 2005/010850 A1